



DEPARTMENT OF THE ARMY  
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX  
75 6TH AVENUE  
FORT KNOX, KENTUCKY 40121-5717

REPLY TO  
ATTENTION OF:

Expires 30 March 2009

IMSE-KNX-IMO

30 March 2007

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters  
Commanders, Fort Knox Partners In Excellence  
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 5-07 – Monitoring of Network Activity by the  
Directorate of Information Management (DOIM)

1. References.

- a. DODD 8500.1, Information Assurance (IA), 24 October 2002.
- b. DODI 8500.2, Information Assurance (IA) Implementation, 6 February 2003.
- c. AR 25-2, Information Assurance, 14 November 2003.
- d. AR 25-1, Army Knowledge Management and Information Technology, 15 July 2005.

2. The use of DOD and other government e-mail and computer systems (including the Internet) is limited to conducting official business or other authorized uses. Commanders and supervisors at all levels will educate employees on authorized and unauthorized uses of government computer systems.

3. All Fort Knox computer users must consent to monitoring of computer activity by clicking OK on the DOD banner before connection to the NIPRNET/INTERNET. They must read and sign the Fort Knox Acceptable Use Policy, FK Form 5063. It is the Information Assurance Security Officer's (IASO's) responsibility to maintain signed copies for all users.

4. Inappropriate activity is defined as any use of government computer systems in a way that would reflect adversely on DOD or the Army. Listed below are examples of inappropriate activity:

- a. Content involving pornography or access to pornographic web sites.
- b. Chain-mail messages.
- c. Unofficial advertising.

IMSE-KNX-IMO

SUBJECT: Fort Knox Policy Memo No. 5-07 – Monitoring of Network Activity by the Directorate of Information Management (DOIM)

- d. Soliciting or selling via e-mail.
- e. Peer-to-peer (P2P).
- f. Other uses incompatible with public service.

The DOIM employs devices/programs to monitor the network for unusual/inappropriate activity. When inappropriate or unauthorized activity is detected emanating from a government information system, a member of the DOIM Information Assurance office will contact the user's IASO/Information Management Officer and commander/director; Fort Knox Designated Approving Authority; Director, DOIM; and Chief, Information/Personnel Security Branch, DPTMS via e-mail outlining the content found and the appropriate steps that need to be taken in order for the user and government information system to be allowed back on the network.

5. Point of contact is the Information Assurance Manager, at 624-5782.

FOR THE COMMANDER:



MARK D. NEEDHAM  
COL, AR  
Garrison Commander

DISTRIBUTION:

A